JOURNAL OF COMBINATORIAL THEORY (B) **19**, 239–255 (1975)

Perfect Codes in the Graphs O_k

P. HAMMOND AND D. H. SMITH

Department of Mathematics and Computer Science, Glamorgan Polytechnic, Treforest, Wales, U.K.

Communicated by W. T. Tutte

Received June 26, 1974

In this paper we consider the existence of perfect codes in the infinite class of distance-transitive graphs O_k. Perfect 1-codes correspond to certain Steiner systems and necessary conditions for the existence of such a code are satisfied if $k + 1$ is prime. We give some nonexistence results for perfect 2-, 3-, and 4-codes and for perfect e-codes in general, including a lower bound for k in terms of e.

The notion of a perfect code has been generalized to the class of distance-transitive graphs by Biggs [1] and to association schemes by Delsarte [3]. Both authors prove a generalization of the theorem of Lloyd [7]. In this paper we shall be concerned with perfect codes in the important infinite class of distance-transitive graphs O_k.

PERFECT CODES IN DISTANCE-TRANSITIVE GRAPHS

We use the notation, definitions, and basic results of [1]. In particular, a simple connected graph with distance function ∂ is said to be *distance-transitive* if, whenever u, v, x, y are vertices satisfying $\partial(u, v) = \partial(x, y)$, then there is an automorphism g of the graph such that $g(u) = x$ and $g(v) = y$. Γ denotes a distance-transitive graph of diameter d and valency k with $|V\Gamma| = n$. Γ has adjacency matrices $A_0, A_1, \ldots, A_d$ and intersection matrices $B_0, B_1, \ldots, B_d$ (i.e., if u and w are vertices of Γ such that $\partial(u, w) = j$, then $(B_f)_{ij} = |\{v \in V\Gamma \mid \partial(u, v) = f, \partial(w, v) = i\}|$). For any vertices u and v such that $\partial(u, v) = i$, we define

$$\Gamma_i(u) = \{w \mid \partial(w, u) = i\},$$

$$k_i = |\Gamma_i(u)|,$$

$$c_i = |\Gamma_{i-1}(u) \cap \Gamma_1(v)|,$$
$$a_i = |\Gamma_i(u) \cap \Gamma_1(v)|,$$
$$b_i = |\Gamma_{i+1}(u) \cap \Gamma_1(v)|.$$

The intersection matrix $B = B_1$ is a tridiagonal matrix with main diagonals given by the intersection array

$$\begin{Bmatrix} * & 1 & c_2 & \cdots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \cdots & a_{d-1} & a_d \\ k & b_1 & b_2 & \cdots & b_{d-1} & * \end{Bmatrix}.$$

Let

$$\mathbf{v}(\lambda) = [v_0(\lambda), v_1(\lambda),..., v_d(\lambda)]^t, \qquad \text{where} \qquad v_0(\lambda) = 1, \quad v_1(\lambda) = \lambda,$$
$$c_{i+1}v_{i+1}(\lambda) + (a_i - \lambda)\, v_i(\lambda) + b_{i-1}v_{i-1}(\lambda) = 0 \qquad (i = 1, 2,..., d-1).$$

Then $v_i(\lambda)$ is a polynomial in λ of degree i. Clearly, if λ is an eigenvalue of B, then $\mathbf{v}(\lambda)$ is the corresponding eigenvector. As shown in [1], $v_i(B) = B_i$.

Let $\Sigma_e(v) = \{u \in V\Gamma \mid \partial(u, v) \leqslant e\}$ and $|\Sigma_e| = |\Sigma_e(v)|$. A *perfect e-code in Γ* is a subset C of $V\Gamma$ such that the sets $\Sigma_e(c)$ $(c \in C)$ form a partition of $V\Gamma$.

Since $\mathbf{k} = [1, k, k_2,..., k_d]^t$ is the eigenvector of B corresponding to eigenvalue k, $v_i(k) = k_i$. Hence if $x_i(\lambda) = v_0(\lambda) + v_1(\lambda) + \cdots + v_i(\lambda)$, we have $x_e(k) = |\Sigma_e|$, $x_d(k) = |V\Gamma|$. We can express the sphere packing condition as $x_e(k)$ divides $x_d(k)$. The main result of [1] is that in the ring $\mathbb{Q}(\lambda)$, $x_e(\lambda)$ divides $x_d(\lambda)$ (which we shall call the polynomial condition), or, alternatively, the e zeros of $x_e(\lambda)$ are eigenvalues of Γ. This latter result generalizes Lloyd's theorem.

In the following lemma we consider the vector

$$\mathbf{p}(C) = [p_0(C), p_1(C),..., p_d(C)]^t$$

where, if $z \in C$, $p_i(C) = |\{u \in C \mid u \in \Gamma_i(z)\}|$. Since in the case of binary perfect codes $p_i(C)$ is the number of code vectors of weight i we shall refer to $\mathbf{p}(C)$ as the *weight vector* of C.

LEMMA 1. *If Γ contains a perfect e-code, C, then $\mathbf{p}(C)$ is a vector of non-negative integers such that $\hat{S}_e\mathbf{p}(C) = \mathbf{k}$, where $\hat{S}_e = B_0 + B_1 + \cdots + B_e = x_e(B)$, $\mathbf{k} = [k_0, k_1,..., k_d]^t$.*

Proof. It follows from the definition of a perfect e-code that if $\mathbf{c}$ is the representative column vector of C, that is, $(\mathbf{c})_v = 1$ if v belongs to C, $(\mathbf{c})_v = 0$ otherwise, then $S_e\mathbf{c} = \mathbf{u}$, where $\mathbf{u} = [1, 1,..., 1]^t$ and $S_e =$

$A_0 + A_1 + \cdots + A_e$. If we fix a vertex z and let T be the $(d+1) \times n$ matrix defined by

$$(T)_{iu} = \begin{cases} 1 & \text{if } \partial(z, u) = i, \\ 0 & \text{otherwise,} \end{cases}$$

then, as in [1], $TS_e = \hat{S}_e T$.

Thus $\hat{S}_e T\mathbf{c} = TS_e\mathbf{c} = T\mathbf{u}$. Also,

$$(T\mathbf{c})_i = \sum_{u \in V\Gamma} T_{iu}(\mathbf{c})_u = \sum_{u \in C} T_{iu} = |\{u \in C \mid u \in \Gamma_i(z)\}| = p_i(C).$$

Since $(T\mathbf{u})_i = |\{u \mid \partial(z, u) = i\}| = |\Gamma_i(z)| = k_i$, we have $\hat{S}_e\mathbf{p}(C) = \mathbf{k}$. ∎

If $z \in C$ we see that $p_0(C) = 1$, $p_1(C) = p_2(C) = \cdots = p_{2e}(C) = 0$. By choosing vertices $u_0, u_1, \ldots, u_e$ such that $\partial(z, u_i) = i$ $(1 \leqslant i \leqslant e)$, we can find automorphisms $g_0, g_1, \ldots, g_e$ of Γ such that $g_i(z) = u_i$ $(0 \leqslant i \leqslant e)$. Associated with each of these automorphisms g_i is the "shifted" perfect e-code $C_i = g_i(C)$. Clearly, $p_j(C_i) = [\mathbf{p}(C_i)]_j = \delta_{ij}$ for $i, j \in \{0, 1, \ldots, e\}$ and so the vectors $\mathbf{p}(C_0), \mathbf{p}(C_1), \ldots, \mathbf{p}(C_e)$ are linearly independent.

LEMMA 2. *If Γ contains a perfect e-code then* $\dim(\ker \hat{S}_e) = e$.

Proof. This is essentially contained in [1, Lemma 2 and the Theorem of Section 4].

THEOREM 1. *If Γ contains a perfect e-code C with shifted codes $C_1, C_2, \ldots, C_e$ and if $\mathbf{p}(C_i)$ is the weight vector associated with the code C_i, then*

$$\mathbf{k} = \sum_{i=0}^{e} k_i \mathbf{p}(C_i).$$

Proof. $\mathbf{k}$ is an eigenvector of B associated with the eigenvalue k. Thus $\hat{S}_e\mathbf{k} = x_e(B)\mathbf{k} = x_e(k)\mathbf{k} = |\Sigma_e|\,\mathbf{k}$. Using Lemma 1, we obtain $\hat{S}_e\mathbf{k} = |\Sigma_e|\,\hat{S}_e\mathbf{p}(C)$ and so $\mathbf{k} - |\Sigma_e|\,\mathbf{p}(C) \in \ker(\hat{S}_e)$. It follows from the linear independence of the set $\{\mathbf{p}(C_0), \mathbf{p}(C_1), \ldots, \mathbf{p}(C_e)\}$ that $\{\mathbf{p}(C_1) - \mathbf{p}(C), \mathbf{p}(C_2) - \mathbf{p}(C), \ldots, \mathbf{p}(C_e) - \mathbf{p}(C)\}$ is a set of linearly independent vectors. Since $\hat{S}_e(\mathbf{p}(C_i) - \mathbf{p}(C)) = \hat{S}_e\mathbf{p}(C_i) - \hat{S}_e\mathbf{p}(C) = \mathbf{k} - \mathbf{k} = \mathbf{0}$ $(1 \leqslant i \leqslant e)$ and $\dim \ker \hat{S}_e = e$, the set $\{\mathbf{p}(C_1) - \mathbf{p}(C), \ldots, \mathbf{p}(C_e) - \mathbf{p}(C)\}$ forms a basis of $\ker \hat{S}_e$. Hence

$$\mathbf{k} - |\Sigma_e|\,\mathbf{p}(C) = \sum_{i=1}^{e} \alpha_i(\mathbf{p}(C_i) - \mathbf{p}(C)),$$

and so

$$\mathbf{k} = \left(|\,\Sigma_e\,| - \sum_{i=1}^{e} \alpha_i\right) \mathbf{p}(C) + \sum_{i=1}^{e} \alpha_i \mathbf{p}(C_i).$$

Equating the first $e + 1$ components gives $|\,\Sigma_e\,| - \sum_{i=1}^{e} \alpha_i = 1$, $k_i = \alpha_i$ $(1 \leqslant i \leqslant e)$ and the result follows. ∎

In the above theorem we proved

$$\hat{S}_e(\mathbf{k} - |\,\Sigma_e\,|\,\mathbf{p}(C)) = 0,$$

which can be written $\hat{S}_e(\hat{S}_e - |\,\Sigma_e\,|\,I)\,\mathbf{p}(C) = 0$. This equation is sometimes more easily applied when computing the weight vector.

Notice that if Γ has $k_d < k_i$ $(i = 1,..., e)$, then Theorem 1 implies that $p_d(C_0) = k_d$. In particular, for an antipodal distance-transitive graph it is known that $k_d < k_i$ $(i = 1,..., e)$ and so if $u \in C_0$ every vertex of $\Gamma_d(u)$ is in C_0. This has been proved independently by O. Heden.

The Graphs O_k

The k-valent graph O_k $(k \geqslant 2)$ has $\binom{2k-1}{k-1}$ vertices indexed by the $(k-1)$-subsets of the set $\{1, 2,..., 2k-1\}$. Two vertices are joined by an edge if and only if their indexing sets are disjoint. O_k has intersection array

$$\left\{\begin{matrix} * & 1 & 1 & 2 & 2 & \cdots & [(k-1)/2] & [k/2] \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & [(k+1)/2] \\ k & k-1 & k-1 & k-2 & k-2 & \cdots & k-[(k-1)/2] & * \end{matrix}\right\}$$

and the eigenvalues of the intersection matrix of O_k are k, $-(k-1)$, $k-2,..., (-1)^{k+1}$. The indexing sets of u and any vertex $v \in \Gamma_i(u)$ have $(i-1)/2$ elements in common if i is odd and $k - 1 - (i/2)$ if i is even.

Using the graph O_k we can construct another distance-transitive graph $2 \cdot O_k$. The k-valent graph $2 \cdot O_k$ has $2\binom{2k-1}{k-1}$ vertices indexed by the sets (x, i), where x is a $(k-1)$-subset of $\{1, 2,..., 2k-1\}$ and $i \in \{0, 1\}$. Two vertices (x, i), (y, j) are adjacent if and only if $x \cap y = \varnothing$ and $i \neq j$. $2 \cdot O_k$ has intersection array

$$\left\{\begin{matrix} * & 1 & 1 & 2 & 2 & \cdots & k-1 & k-1 & k \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ k & k-1 & k-1 & k-2 & k-2 & \cdots & 1 & 1 & * \end{matrix}\right\}$$

and the eigenvalues of the intersection matrix are $\pm k$, $\pm(k-1),..., \pm 1$.

THEOREM 2. *O_k contains a perfect e-code if and only if $2 \cdot O_k$ contains a perfect e-code.*

Proof. Suppose that O_k contains a perfect e-code C. Then

$$|C| = \binom{2k-1}{k-1} \Big/ |\Sigma_e|.$$

We show that $C \times \{0, 1\}$ is a perfect e-code in $2 \cdot O_k$. Let ∂' denote distance in $2 \cdot O_k$. If (x, i) and (y, j) are elements of $C \times \{0, 1\}$, then since $x, y \in C$, $\partial'((x, i), (y, j)) \geqslant \partial(x, y) \geqslant 2e + 1$. Since $|\Sigma_e|$ is the same in both cases,

$$|C \times \{0, 1\}| = 2 \binom{2k-1}{k-1} \Big/ |\Sigma_e|$$

and the code is perfect.

Conversely, suppose that $2 \cdot O_k$ has a perfect e-code C. From Theorem 1, $\mathbf{k} = \sum_{i=0}^{e} k_i \mathbf{p}(C_i)$, where C_i $(1 \leqslant i \leqslant e)$ are the shifted codes associated with C. The last component of this equation gives $1 = k_d = \sum_{i=0}^{e} k_i p_d(C_i)$, but $k_i > 1$ for $1 \leqslant i \leqslant e$ and so $p_d(C_0) = p_d(C) = 1$. This implies that if Z is a code point then the antipodal point Z' such that $\partial(Z, Z') = d$ is a code point and so by identifying pairs of antipodal code points we can obtain a perfect code in O_k. ∎

THE EXISTENCE OF PERFECT CODES IN O_k

a. *Perfect 1-Codes*

Perfect 1-codes are known in O_4 and O_6 and the codes form Steiner systems $1; (2, 3, 7)$ and $1; (4, 5, 11)$, respectively. We shall show in Theorem 3 that any perfect 1-code in O_k is a Steiner system $1; (k-2, k-1, 2k-1)$ and a Steiner system $1; (k-2, k-1, 2k-1)$ is a perfect 1-code in O_k.

LEMMA 3. *If a $1; (k-2, k-1, 2k-1)$ Steiner system exists, then $k+1$ is prime.*

Proof. A well-known necessary condition for the existence of a $\lambda; (t, d, n)$ design is that $\binom{d-h}{t-h}$ divides $\lambda\binom{n-h}{t-h}$ $(h = 0, 1, \ldots, t-1)$.

In this case we have $(k-1-h)$ divides $(2k-1-h)(2k-2-h) \cdots (k+2)/(k-2-h)!$ $(h = 0, 1, \ldots, k-3)$. Let p be any prime between 2 and $k-1$, then for $h = k-p-1$, p divides $(k+p)(k+p-1) \cdots (k+2)/(p-1)!$ and so p does not divide $k+1$. Since $k \geqslant 2$, k does not divide $k+1$ and the result follows.

THEOREM 3. *Let C be a subset of the vertices of O_k. The labels of the vertices of C form a* $1; (k-2, k-1, 2k-1)$ *Steiner system if and only if C is a perfect* 1-*code.*

Proof. (1) Suppose that O_k contains a perfect 1-code C and that $\mathscr{C}$ is the system of $(k-1)$-subsets of the ground set $\{1, 2,..., 2k-1\}$ which label C. Since any pair of elements of C are at least distance 3 apart, their labeling sets cannot have $k-2$ elements in common. Hence each $(k-2)$-subset of the ground set is contained in at most one element of $\mathscr{C}$. Since $|C|(k-1) = \binom{2k-1}{k-2}$, it follows that each $(k-2)$-subset is in fact contained in exactly one element of $\mathscr{C}$.

(2) Conversely, suppose that $\mathscr{C}$ is a $1; (k-2, k-1, 2k-1)$ Steiner system. We show that the set of vertices C labeled by blocks of $\mathscr{C}$ form a perfect 1-code in O_k. There are $\binom{2k-1}{k-1}/(k+1)$ such vertices; we show that the minimum distance between them is 3. Since no two blocks of $\mathscr{C}$ have $k-2$ elements in common, no two vertices of C can be at distance 2. We now show that no two blocks of $\mathscr{C}$ are disjoint, in order to show that no two vertices can be at distance 1. Without loss of generality we can assume that $\{1, 2,..., k-1\}$ is a block of $\mathscr{C}$ and show that every other block contains at least one of the elements of $\{1, 2,..., k-1\}$.

We use the notation $N(a \cup b \cup \cdots \cup f)$, $N(a \cap b \cap \cdots \cap f)$ to denote the number of blocks of $\mathscr{C}$ containing the elements a or b or $\cdots$ or f, a and b and $\cdots$ and f respectively. By the principle of inclusion and exclusion we have

$$\begin{aligned} N(1 \cup 2 \cup \cdots \cup k-1) = {} & N(1) + N(2) + \cdots + N(k-1) \\ & - N(1 \cap 2) - \cdots - N(k-2 \cap k-1) + \cdots \\ & + (-1)^k N(1 \cap 2 \cap \cdots \cap k-1). \end{aligned}$$

Let r_j denote the number of blocks of $\mathscr{C}$ containing j particular elements of $\{1, 2,..., k-1\}$.

$$r_j = \frac{(2k-j-1)!}{(k-j-1)!\,(k+1)!} = \frac{1}{(k-j-1)}\binom{2k-j-1}{k-j-2} \qquad [2, \text{p. } 50].$$

Hence

$$\begin{aligned} & N(1 \cup 2 \cup \cdots \cup k-1) \\ & \quad = \sum_{s=1}^{k-2} (-1)^s \binom{k-1}{s}\binom{k+s}{s-1}\frac{1}{s} + 1 \\ & \quad = 1 - \left[\sum_{s=1}^{k-2} (-1)^{k-1-s} \binom{k-1}{s}\binom{k+s}{s}\right]\frac{1}{k+1}, \end{aligned}$$

since $k + 1$ is prime. By equating the coefficients of x^{k-1} in $(1 + x)^{k-1}(1 + x)^{-k-1}$ and $(1 + x)^{-2}$, we obtain

$$\sum_{s=1}^{k-1} (-1)^{k-1-s} \binom{k-1}{s}\binom{k+s}{s} = k + (-1)^k.$$

Thus

$$N(1 \cup 2 \cup \cdots \cup k - 1)$$
$$= 1 - \left[k + 1 - \binom{2k-1}{k-1}\right] \frac{1}{k+1} = \frac{1}{k+1} \binom{2k-1}{k-1} = | C |$$

and so no two blocks are disjoint. ∎

The weight vector equation $\hat{S}_e\mathbf{p}(C) = \mathbf{k}$ for a 1-code in O_k gives $(B + I)\mathbf{p} = \mathbf{k}$. If $p_i = [\mathbf{p}]_i$, then the component equations are

$$k_{2r} = (k - r)\, p_{2r-1} + p_{2r} + (r + 1)\, p_{2r+1} \quad (r = 0, 1,\ldots, [(k + 1)/2] - 1)$$
$$k_{2r+1} = (k - r)\, p_{2r} + p_{2r+1} + (r + 1)\, p_{2r+2} \quad (r = 0, 1,\ldots, [(k - 1)/2]).$$

Assuming $p_0 = 1$, these two equations, together with $(k - r)\, k_{2r} = (r + 1)\, k_{2r+1}$ enable us to prove inductively that

$$p_{2r} = ((k - r)/r)\, p_{2r-1} \qquad (r = 1, 2,\ldots, [(k + 1)/2] - 1).$$

It then follows by counting Γ_{2r} that

$$p_{2r+1} = (k_{2r}/(r + 1)) - p_{2r} \qquad (r = 0, 1,\ldots, [(k - 1)/2]).$$

Manipulating these two expressions, we can obtain an explicit form for p_{2r}:

$$p_{2r} = \frac{(-1)^{r-1}}{(k+1)} \binom{k-1}{r} \sum_{i=1}^{r-1} (-1)^i \binom{k+1}{i+1}$$
$$(r = 0, 1,\ldots, [(k + 1)/2] - 1).$$

For $k + 1$ prime each term in the summation will be divisible by $k + 1$ and hence p_{2r} $(r = 0, 1,\ldots, [(k + 1)/2] - 1)$ are integral and positive. Since $k_{2r+1} = ((k - r)/(r + 1))\, k_{2r}$ and $k + 1$ is prime, $(r + 1) \mid k_{2r}$ and we have that p_{2r+1} $(r = 0, 1,\ldots, [(k - 1)/2])$ are positive integers. A similar result holds if $p_0 = 0, p_1 = 1$.

Hence we have shown, independently of the existence of a perfect 1-code, that the weight vector equation always has positive integer solutions if $k + 1$ is prime. This may be considered as supporting evidence for the possible existence of other perfect 1-codes in O_k, although

Theorem 3, combined with the conjecture that no t-designs exist with $t > 5$, would indicate that no other perfect 1-codes in O_k can exist.

b. *Perfect 2-Codes*

If O_k contains a perfect 2-code, then by the polynomial condition the roots of $x_2(\lambda)$ must belong to the set $\{-(k-1), k-2, \ldots, (-1)^{k+1}\}$. Since $x_2(\lambda) = \lambda^2 + \lambda - (k-1)$, the roots will be of the form a, $-a-1$, where $a > 0$ and $k - 1 = a(a+1)$. Hence k is odd and so a is odd, which gives

$$k - 1 = (2m-1)\,2m \ (m > 0), \qquad \text{so} \qquad k = 1 - 2m + 4m^2 \ (m > 0).$$

For $m = 1$ we obtain the trivial perfect 2-code in O_3, so we assume for the rest of this section that $k \geqslant 13$.

From the weight vector equation for 2-codes in O_k, $\hat{S}_2\mathbf{p}(C) = (B^2 + B - (k-1)I)\,\mathbf{p}(C) = \mathbf{k}$ we can obtain explicit expressions for the components of $\mathbf{p}(C)$. In particular, if $p_0 = 1$, we have

$$p_{10} = \frac{k(k-1)^2\,(k-3)(k-5)(k^3 - 15k^2 + 87k - 181)}{5^2 \cdot 4^2 \cdot 3^2 \cdot 2^2}$$

and since $k^3 - 15k^2 + 87k - 181$ is never divisible by 5, 5^2 divides $k(k-1)^2(k-3)(k-5)$. Since $k = 1 - 2m + 4m^2$, 5^2 divides $(4m^2 - 2m + 1)\,m^2(2m-1)^2(2m+1)(m-1)(4m^2 - 2m - 4)$. But $4m^2 - 2m + 1$ and $4m^2 - 2m - 4$ are never divisible by 5 so that 5^2 divides $m^2(2m-1)^2(2m+1)(m-1)$. We have four possibilities:

(1) $m \equiv 0 \bmod 5$, $\quad k = 100r^2 + 190r + 91 \quad (r = 0, 1, \ldots)$

(2) $m \equiv 3 \bmod 5$, $\quad k = 100r^2 + 110r + 31 \quad (r = 0, 1, \ldots)$

(3) $m \equiv 1 \bmod 25$, $\quad k = 2500r^2 + 150r + 3 \quad (r = 1, 2, \ldots)$

(4) $m \equiv 12 \bmod 25$, $\quad k = 2500r^2 + 2350r + 553 \quad (r = 0, 1, \ldots)$

We can eliminate some of these cases by using the sphere packing condition: $1 + k^2 \mid \binom{2k-1}{k-1}$, where $k = 1 - 2m + 4m^2$ and so $1 + k^2 = 2(4m^2 + 1)(m^2 + (m-1)^2)$. Let p denote $m^2 + (m-1)^2$. Since $m \geqslant 3$ we have $5p > 2k - 1$, $4p < 2k - 1$, $3p > k$, $2p < k - 1$. Consequently, when p is prime it is relatively prime to

$$\binom{2k-1}{k-1} = \frac{(2k-1)\cdots(k+1)}{(k-1)\cdots 1},$$

and so the sphere packing condition will fail to hold.

Case 1. $m \equiv 0 \bmod 5$. The first value of m for which p is nonprime is $m = 45$, so for k of the form $k = 100r^2 + 190r + 91$, O_k does not contain a perfect 2-code for $k < 9901$.

Case 2. $m \equiv 3 \bmod 5$. The first value of m for which p is nonprime is $m = 28$, so for k of the form $100r^2 + 110r + 31$, O_k does not contain a nontrivial perfect 2-code for $k < 3081$.

Case 3. $m \equiv 1 \bmod 25$. For $r = 1$, $m = 26$, $p = 1301$, which is prime, and so for $k = 2500r^2 + 150r + 3$, O_k does not contain a nontrivial perfect 2-code for $k < 10303$.

Case 4. $m \equiv 12 \bmod 25$. For $r = 0$, $m = 12$, $p = 265 = 5.53$ but in fact 53 is relatively prime to $\binom{1105}{552}$. Hence for k of the form $2500r^2 + 2350r + 553$, O_k does not contain a perfect 2-code for $k < 5403$.

Combining these four cases, we have the result that there are no nontrivial perfect 2-codes in O_k for $k < 3081$. We can deduce further bounds by looking at other components of the weight vector.

c. *Perfect* 3-*Codes*

From the eigenvector sequence we obtain

$$x_3(\lambda) = \tfrac{1}{2}(\lambda^3 + 2\lambda^2 - (2k-3)\lambda - 2(k-1)).$$

If O_k contains a perfect 3-code, then the roots of $x_3(\lambda)$ are members of the set $\{-(k-1), k-2,..., (-1)^{k+1}\}$. Obviously, -1 is a root of $x_3(\lambda)$ so k is even and the other roots are of the form $-(2p-1)$, $2s$, where $p > 0$, $s > 0$. The sum and product of the roots give $p - s = 1$ and $(2p-1)s = k-1$. Since k is even, s is odd and so p is even. If $p = 2m$ $(m > 0)$, we obtain $k = 1 + (4m-1)(2m-1) = 2(4m^2 - 3m + 1)$ $(m > 0)$. The case $m = 1$, $k = 4$ corresponds to the trivial perfect 3-code in O_4. We assume $m > 1$. From the weight vector equation we find that if $p_0 = 1$,

$$p_{11} = k(k-1)^2(k-2)(k-4)(k^3 - 22k^2 + 197k - 584)/2^6 \cdot 3^3 \cdot 5^2,$$

and since k is even, $2^6 \mid k(k-2)(k-4)(k^3 - 22k^2 + 197k - 584)$. Let $q = 4m^2 - 3m + 1$ so that $k = 2q$ and then $2^2 \mid q(q-1)(q-2)(4q^3 - 44q^2 + 197q - 292)$. Hence either q is even or $q \equiv 1 \bmod 4$ and so m is odd or $m \equiv 0 \bmod 4$. This gives two possibilities for k:

(1) $k = 32r^2 + 20r + 4 \qquad (r = 1, 2,...)$,

(2) $k = 128r^2 - 24r + 2$.

d. *Perfect* 4-*Codes*

Since $x_4(\lambda) = \frac{1}{4}(\lambda^4 + 2\lambda^3 + \lambda^2(7 - 4k) + \lambda(6 - 4k) + 2(k-1)(k-2))$, $x_4(\gamma) = 0$ implies that $x_4(-\gamma - 1) = 0$ so we can assume that the roots of $x_4(\lambda)$ are of the form γ, δ, $-\gamma - 1$, $-\delta - 1$ where $\gamma, \delta > 0$. Then

$$\gamma(\gamma + 1) + \delta(\delta + 1) = 4k - 6,$$
$$\gamma(\gamma + 1)\, \delta(\delta + 1) = 2(k-1)(k-2),$$

and if $\alpha = \gamma(\gamma + 1)$ then $\alpha^2 - (4k - 6)\alpha + 2(k-1)(k-2) = 0$, and so $\alpha = 2k - 3 \pm (2k^2 - 6k + 5)^{1/2}$.

If O_k contains a perfect 4-code, α is integral and $2k^2 - 6k + 5 = r^2$ for some integer $r > 1$, that is, $(k-2)^2 + (k-1)^2 = r^2$. The first positive integer solution for k is $r = 5$, $k = 5$, which corresponds to the trivial code in O_5. The next solution is $k = 22$, $r = 29$ so we shall assume now that $k \geqslant 22$.

The equation $(k-2)^2 + (k-1)^2 = r^2$ has general solution as follows [4, p. 190].

(1) *k even.* $k - 2 = 2ab$, $k - 1 = a^2 - b^2$, $r = a^2 + b^2$, so that $a^2 - 2ab - b^2 - 1 = 0$, which gives $a = b + (1 + 2b^2)^{1/2}$. Letting $x = a - b$, the equation $x^2 = 1 + 2b^2$ $(x > 0,\ b > 0)$ has general solution given by $x_n = (1 + \sqrt{2})^{2n} - b\sqrt{2}$ $(n = 1, 2,...)$ [4, p. 210] and so $k = 2 + 2b(b(1 - \sqrt{2}) + (1 + \sqrt{2})^{2n})$ $(n = 1, 2,...)$.

(2) *k odd.* $k - 1 = 2ab$, $k - 2 = a^2 - b^2$, $r = a^2 + b^2$, which gives $k = 1 + 2b(b + x_n)$, where b, x_n satisfy $x_n{}^2 = 2b^2 - 1$ and $x_n + b\sqrt{2} = (1 + \sqrt{2})^{2n+1}$ $(n = 1, 2,...)$.

The first four possibilities for k are 22, 121, 698, 4061. From the weight vector equation we obtain for $p_0 = 1$,

$$p_{11} = k(k-1)^2(k-2)^2(k-5)(k-17)/6 \cdot 5^2 \cdot 4^2 \cdot 3^2.$$

We can rule out the first three cases, since p_{11} is an integer, so O_k does not contain a nontrivial perfect 4-code for $k < 4061$.

e. *Perfect e-Codes with e Odd*

LEMMA 4. *Let $v_0(\lambda), v_1(\lambda),..., v_d(\lambda)$ be the eigenvector sequence associated with O_k. Then for $m = 0, 1,..., [(d+1)/2] - 1$,*

$$x_{2m+1}(-1) = \sum_{i=0}^{2m+1} v_i(-1) = 0.$$

Proof. The eigenvector sequence gives the following pair of equations.

$$(k-m)\,v_{2m}(\lambda)+(m+1)\,v_{2m+2}(\lambda)=\lambda v_{2m+1}(\lambda) \qquad (m=0,1,\ldots,[(d+1)/2]-1),$$

$$(k-m-1)\,v_{2m+1}(\lambda)+(m+2)\,v_{2m+3}(\lambda)=\lambda v_{2m+2}(\lambda) \qquad (m=0,1,\ldots,[d/2]-1).$$

We proceed by induction on m. It is easily shown that $x_1(-1)=x_3(-1)=0$, so we suppose that $x_{2m+1}(-1)=0$. Substituting $\lambda=-1$ in the equations above gives

$$(k-m)\,v_{2m}(-1)+(m+1)\,v_{2m+2}(-1)=-v_{2m+1}(-1), \tag{1}$$

$$(k-m-1)\,v_{2m+1}(-1)+(m+2)\,v_{2m+3}(-1)=-v_{2m+2}(-1), \tag{2}$$

and we also have

$$0=x_{2m+1}(-1)=v_{2m}(-1)+v_{2m+1}(-1). \tag{3}$$

Equations (3) and (1) give

$$(m+1)\,v_{2m+2}(-1)=-(k-m-1)\,v_{2m}(-1). \tag{4}$$

Equations (3) and (2) give

$$\begin{aligned}(m+2)\,v_{2m+3}(-1)&=-v_{2m+2}(-1)+(k-m-1)\,v_{2m}(-1)\\&=((k-m-1)/(m+1))(m+2)\,v_{2m}(-1),\end{aligned}$$

so we have

$$v_{2m+3}(-1)=((k-m-1)/(m+1))\,v_{2m}(-1). \tag{5}$$

Comparing (4) and (5), we have $v_{2m+2}(-1)=-v_{2m+3}(-1)$, so $x_{2m+3}(-1)=0$ and the result follows by induction. ∎

THEOREM 4. *If O_k contains a perfect e-code and e is odd, then k is even.*

Proof. If O_k contains a perfect e-code with e odd, then -1 is a root of $x_e(\lambda)$ and so -1 is an eigenvalue of O_k. The eigenvalue of O_k of smallest absolute value is $(-1)^{k+1}$ and so k must be even. ∎

f. *A Lower Bound*

THEOREM 5. *If a non-trivial perfect e-code exists in O_k then $k \geqslant (e^2 + 4e + 2)/2$ (e even) and $k \geqslant (e^2 + 4e + 3)/2$ (e odd).*

Proof of Case 1. $e = 2m$. We assume that $p_1, p_2, \ldots, p_d$ are not all zero. Notice first that $\partial(x, y) = e - 2, e - 1, e$ according as the labels of x and y have $k - m, m - 1, k - m - 1$ elements in common. Also, the labels of Γ_0 and $\Gamma_{e+1}, \Gamma_{e+2}, \Gamma_{e+3}$ have, respectively, $m, k - 2 - m, m + 1$ elements in common. Similarly, the labels of Γ_0 and $\Gamma_{2e+1}, \Gamma_{2e+2}, \Gamma_{2e+3}$ have, respectively, $2m, k - 2 - 2m, 2m + 1$ elements in common.

First we count in two ways the vertices of Γ_{e+1}. Each vertex of Γ_{e+1} is distance e from exactly one code point of Γ_{2e+1}. Let the vertex of Γ_{e+1} have q elements of the labeling set in common with Γ_0 and the code point of Γ_{2e+1}:

$$k_{e+1} = \binom{k-1}{m}\binom{k}{k-1-m}$$

$$= p_{2e+1} \sum_{q=0}^{m} \binom{2m}{q}\binom{k-1-2m}{m-q}\binom{k-1-2m}{k-1-m-q}\binom{2m+1}{q}$$

$$= p_{2e+1} \binom{2m}{m}\binom{2m+1}{m}.$$

Similarly, counting in two ways the vertices of Γ_{e+2}:

$$k_{e+2} = \binom{k-1}{m+1}\binom{k}{k-m-1}$$

$$= p_{2e+2} \sum_{q=0}^{k-2-2m} \binom{k-2-2m}{q}\binom{2m+1}{k-2-m-q}$$

$$\times \binom{2m+1}{k-m-1-q}\binom{k-2m-1}{q-k+2m+2}$$

$$+ p_{2e+1} \sum_{q=0}^{m-1} \binom{2m}{q}\binom{k-1-2m}{m-1-q}\binom{k-1-2m}{k-2-m-q}\binom{2m+1}{q+2}$$

$$= p_{2e+2} \binom{2m+1}{m}\binom{2m+1}{m+1} + p_{2e+1} \binom{2m}{m-1}\binom{2m+1}{m+1}.$$

Combining these equations we have

$$(k - 1 - m)/(m + 1) = (m/(m + 1)) + ((2m + 1)/(m + 1))(p_{2e+2}/p_{2e+1}).$$

Now counting Γ_{e+3} in two ways:

$$k_{e+3} = \binom{k-1}{m+1}\binom{k}{k-m-2}$$

$$= p_{2e+3} \sum_{q=0}^{m+1} \binom{2m+1}{q}\binom{k-2m-2}{m+1-q}\binom{k-2m-2}{k-1-m-q}\binom{2m+2}{q-1}$$

$$+ p_{2e+2} \sum_{q=0}^{m-1} \binom{k-2-2m}{q}\binom{2m+1}{m+1-q}$$

$$\times \binom{2m+1}{m-1-q}\binom{k-1-2m}{k-1-2m+q}$$

$$+ p_{2e+1} \left[\sum_{q=0}^{m+1} \binom{2m}{q}\binom{k-1-2m}{m+1-q}\binom{k-1-2m}{k-m-q}\binom{2m+1}{q-2}\right.$$

$$\left. + \sum_{q=0}^{m+1} \binom{2m}{q}\binom{k-1-2m}{m+1-q}\binom{k-1-2m}{k-1-m-q}\binom{2m+1}{q-1}\right]$$

$$= p_{2e+3} \binom{2m+1}{m+1}\binom{2m+2}{m} + p_{2e+2} \binom{2m+1}{m+1}\binom{2m+1}{m-1}$$

$$+ p_{2e+1} \left[\binom{2m}{m+1}\binom{2m+1}{m-1} + \binom{2m}{m}(k-1-2m)\binom{2m+1}{m-1}\right.$$

$$\left. + \binom{2m}{m+1}\binom{2m+1}{m}\right].$$

Eliminating p_{2e+2} from these equations gives

$$\frac{p_{2e+3}}{p_{2e+1}} = \frac{k^2 - 2k(m^2+3m+1) + (4m^3+10m^2+6m+1)}{(2m+2)(2m+1)},$$

and since $p_{2e+3}/p_{2e+1} \geqslant 0$, $k \leqslant (4m+2)/2$ or $k \geqslant (4m^2+8m+2)/2$, so $k \leqslant e+1$, which corresponds to a trivial code or $k \geqslant (e^2+4e+2)/2$.

Case 2. $e = 2m+1$. Again we assume that $p_1, \ldots, p_d$ are not all zero. In this case $\partial(x, y) = e-2, e-1, e$ according as the labels of x and y have $m-1$, $k-m-1$, m elements in common. Also, the labels of Γ_0 and Γ_{e+1}, Γ_{e+2}, Γ_{e+3} have, respectively, $k-2-m$, $m+1$, $k-3-m$ elements in common. Similarly, the labels of Γ_0 and Γ_{2e+1}, Γ_{2e+2}, Γ_{2e+3} have, respectively, $2m+1$, $k-3-2m$, $2m+2$ elements in common.

The proof goes through in the same way, the relevant equations being

$$\binom{k}{m+1}\binom{k-1}{m+1} = p_{2e+1}\binom{2m+1}{m}\binom{2m+2}{m+1},$$

$$\binom{k}{m+2}\binom{k-1}{m+1} = \binom{2m+2}{m+1}\binom{2m+2}{m} p_{2e+2} + \binom{2m+1}{m+1}\binom{2m+2}{m} p_{2e+1}$$

$$\begin{aligned}\binom{k}{m+2}\binom{k-1}{m+2} = \binom{2m+2}{m}\binom{2m+3}{m+2} p_{2e+3} + \binom{2m+2}{m}\binom{2m+2}{m+2} p_{2e+2} \\ + p_{2e+1}\left[\binom{2m+1}{m-1}\binom{2m+2}{m+2}\right. \\ + (k-2-2m)\binom{2m+1}{m-1}\binom{2m+2}{m+1} \\ \left. + (k-2-2m)\binom{2m+1}{m}\binom{2m+2}{m+2}\right].\end{aligned}$$

Again, eliminating p_{2e+2}, we have

$$\begin{aligned}(2m+2)(2m+3)(p_{2e+3}/p_{2e+1}) = k^2 - (k/2)(2m+6)(2m+2) \\ + \tfrac{1}{2}(2m+2)^2(2m+4),\end{aligned}$$

so $0 \leqslant \{k - [(e+1)(e+3)/2]\}[k-(e+1)]$, and the result follows. ∎

Note. The same method can be used in the classical case of perfect codes in an n-dimensional vector space over GF(q) dealt with by Tietäväinen [8, 9], to show that $n \geqslant e^2/2 + 5e/2 + 1$ $(q > 2)$ and $n \geqslant e^2 + 4e + 2$ $(q = 2)$ [6, Lemma 1]. This has been used by Van Lint to simplify the proof in the case $q = 2$.

g. *Roots of* $x_e(\lambda)$

THEOREM 6.

$$x_{2m}(\lambda) = x_{2m}(-\lambda-1), \qquad m = 0, 1, \ldots, [(d+1)/2] - 1,$$

$$\lambda x_{2m+1}(\lambda) = -(\lambda+1)\, x_{2m+1}(-\lambda-1), \quad m = 0, 1, \ldots, [d/2] - 1.$$

Proof. Three successive components of the eigenvector sequence for O_k give

$$(k-m)\, v_{2m-1}(\lambda) + (m+1)\, v_{2m+1}(\lambda) = \lambda v_{2m}(\lambda), \tag{1}$$

$$(k-m)\, v_{2m}(\lambda) + (m+1)\, v_{2m+2}(\lambda) = \lambda v_{2m+1}(\lambda), \tag{2}$$

$$(k-m-1)\, v_{2m+1}(\lambda) + (m+2)\, v_{2m+3}(\lambda) = \lambda v_{2m+2}(\lambda). \tag{3}$$

Writing $p_i(\lambda) = v_i(\lambda) + v_{i+1}(\lambda)$ and adding (1) and (2), and (2) and (3) gives

$$(k - m)\, p_{2m-1}(\lambda) + (m + 1)\, p_{2m+1}(\lambda) = \lambda p_{2m}(\lambda), \tag{4}$$

$$(k - m)\, p_{2m}(\lambda) + (m + 2)\, p_{2m+2}(\lambda) = (\lambda + 1)\, p_{2m+1}(\lambda). \tag{5}$$

We shall prove the theorem by induction on m. It is not difficult to show that the results $x_{2m}(\lambda) = x_{2m}(-\lambda - 1)$, $\lambda x_{2m+1}(\lambda) = -(\lambda + 1)\, x_{2m+1}(-\lambda - 1)$ hold for $m = 0, 1, 2$. Suppose that the theorem is true for $r \leqslant m$. We must show that

$$x_{2m+2}(\lambda) = x_{2m+2}(-\lambda - 1) \quad \text{and} \quad \lambda x_{2m+3}(\lambda) = -(\lambda + 1)\, x_{2m+3}(\lambda),$$

and since we have the inductive hypothesis it is sufficient to show that

$$p_{2m+1}(\lambda) = p_{2m+1}(-\lambda - 1) \quad \text{and} \quad \lambda p_{2m+2}(\lambda) = -(\lambda + 1)\, p_{2m+2}(-\lambda - 1).$$

Replacing λ by $-\lambda - 1$ in (4) gives

$$\begin{aligned}(k - m)\, p_{2m-1}(-\lambda - 1) &+ (m + 1)\, p_{2m+1}(-\lambda - 1)\\ &= (-\lambda - 1)\, p_{2m}(-\lambda - 1),\end{aligned}$$

which, by the inductive hypothesis, reduces to

$$(k - m)\, p_{2m-1}(\lambda) + (m + 1)\, p_{2m+1}(-\lambda - 1) = \lambda p_{2m}(\lambda).$$

Comparing the last equation with (4) gives $p_{2m+1}(-\lambda - 1) = p_{2m+1}(\lambda)$. Replacing λ by $-\lambda - 1$ in (5) gives

$$(k - m)\, p_{2m}(-\lambda - 1) + (m + 2)\, p_{2m+2}(-\lambda - 1) = -\lambda p_{2m+1}(-\lambda - 1).$$

Multiplying by $-(1 + \lambda)$ and using the inductive hypothesis gives

$$(k - m)\, \lambda p_{2m}(\lambda) - (m + 2)(\lambda + 1)\, p_{2m+2}(-\lambda - 1) = \lambda(\lambda + 1)\, p_{2m+1}(\lambda).$$

Comparing the last equation with (5). λ gives

$$-(\lambda + 1)\, p_{2m+2}(-\lambda - 1) = \lambda p_{2m+2}(\lambda). \quad \blacksquare$$

If $p(\lambda) = x_{2m+1}(\lambda)/(\lambda + 1)$, then the previous theorem shows that

$$p(-\lambda - 1) = x_{2m+1}(-\lambda - 1)/-\lambda = x_{2m+1}(\lambda)/(\lambda + 1) = p(\lambda),$$

and hence for any e, if γ is a root of $x_e(\lambda)$ and $\gamma \neq -1$, then $-\gamma - 1$ is also a root. Let the roots of $x_e(\lambda)$ be denoted by $x_1, x_2, \ldots, x_e$, then

$$x_1 + x_2 + \cdots + x_e = -(\text{coefficient of } \lambda^{e-1} \text{ in } x_e(\lambda))/(\text{coefficient of } \lambda^e).$$

Since $x_e(\lambda) = x_{e-2}(\lambda) + v_{e-1}(\lambda) + v_e(\lambda)$ and $v_i(\lambda)$ is of degree i with no λ^{i-1} term, then

$$\text{the coefficient of } \lambda^{e-1} = x_e^{(e-1)}(0)/(e-1)! = v_{e-1}^{(e-1)}(0)/(e-1)!$$

and

$$\text{the coefficient of } \lambda^{e} = x_e^{(e)}(0)/e! = v_e^{(e)}(0)/e!,$$

where $p^{(e)}(\lambda) = d^e(p(\lambda))/d\lambda^e$. Then

$$x_1 + x_2 + \cdots + x_e = -v_{e-1}^{(e-1)}(0) \cdot e/v_e^{(e)}(0),$$

and from the eigenvector sequence we get

$$(k - [(e-1)/2])\, v_{e-2}(\lambda) + [(e+1)/2]\, v_e(\lambda) = \lambda v_{e-1}(\lambda),$$

so that

$$[(e+1)/2]\, v_e^{(e)}(0) = e v_{e-1}^{(e-1)}(0)$$

and

$$x_1 + x_2 + \cdots + x_e = -[(e+1)/2].$$

Using a similar but longer method we find that

$$x_1 x_2 \cdots x_e = (-1)^{e+[e/2]} \left[\frac{e}{2}\right]! \left[\frac{e+1}{2}\right]! \binom{k-1}{[e/2]}.$$

Combining this with Theorem 6, we see that the roots of $x_e(\lambda)$ have the following product.

$e = 2m$. $x_e(\lambda)$ has roots $\alpha_1, \alpha_2, \ldots, \alpha_m$, $-(1+\alpha_1), -(1+\alpha_2), \ldots, -(1+\alpha_m)$, where $\alpha_i > 0$, $i = 1, 2, \ldots, m$, and

$$\alpha_1 \alpha_2 \cdots \alpha_m (1+\alpha_1)(1+\alpha_2) \cdots (1+\alpha_m) = m!\, m! \binom{k-1}{m}.$$

$e = 2m + 1$. $x_e(\lambda)$ has roots $\alpha_1, \alpha_2, \ldots, \alpha_m$, $-(1+\alpha_1), -(1+\alpha_2), \ldots, -(1+\alpha_m), -1$, where $\alpha_i > 0$, $i = 1, 2, \ldots, m$, and

$$\alpha_1 \alpha_2 \cdots \alpha_m (1+\alpha_1)(1+\alpha_2) \cdots (1+\alpha_m) = m!\, (m+1)! \binom{k-1}{m}.$$

In the classical case of perfect codes the analogous polynomial condition to $x_e(\lambda)$ dividing $x_d(\lambda)$ is that Lloyd's polynomial has roots in a certain set of positive integers. Tietäväinen [8] used the sum and product of the roots of Lloyd's polynomial to prove the nonexistence of unknown perfect

e-codes over a q-ary alphabet. In the proof Tietäväinen makes use of the sphere packing condition, which in this case is that $|\Sigma_e|$ divides $|V| = q^n$, and then uses the fact that $|\Sigma_e|$ is a power of a prime p where $q = p^\alpha$. The sphere packing condition for O_k is that $|\Sigma_e|$ divides $|V| = \binom{2k-1}{k-1}$, which is much more difficult to work with, and for this reason it appears that the same method is not applicable.

It appears that without using this sphere packing condition it is not even possible to deal with any particular value of e completely. For example, in the case $e = 2$, if $k = 4m^2 - 2m + 1$, the existence of the factor $(k - 1) = m(4m - 2)$ in each component p_i $(i \geqslant 2e + 1)$ means that for any fixed value of i, $p_i, p_{i-1}, \ldots, p_{2e+1}$ will be positive integers for some suitable value of m. Similarly, if $e = 3$, we have a factor $(k - 2)$ in each p_i $(i \geqslant 2e + 1)$. Some progress has recently been made in the use of sphere packing conditions in which $|V|$ is not a power of a prime [6] but the condition $|\Sigma_e|$ divides $\binom{2k-1}{k-1}$ appears very much harder than the example given in [6].

References

1. N. L. Biggs, Perfect codes in graphs, *J. Combinatorial Theory, Ser. B* **15** (1973), 289–296.
2. N. L. Biggs, "Finite Groups of Automorphisms," London Math. Soc. Lecture Notes, No. 6, Cambridge University Press, London, 1971.
3. P. Delsarte, An algebraic approach to the association schemes of coding theory, Thesis, Université Catholique de Louvain, 1973.
4. G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 4th ed., Oxford University Press, London/New York, 1960.
5. J. H. van Lint, "Coding Theory," Lecture Notes in Maths. No. 201, Springer–Verlag, New York/Berlin, 1971.
6. J. H. van Lint, Recent results on perfect codes and related topics, Proc. Advanced Study Institute, Nijenrode Castle, Breukelen (Math. Centre Tracts 55), 1974, pp. 158–178.
7. S. P. Lloyd, Binary block coding, *Bell System Tech. J.* **36** (1957), 517–535.
8. A. Tietäväinen, On the non-existence of perfect codes over finite fields, *SIAM J. Appl. Math.* **24** (1973), 88–96.
9. A. Tietäväinen and A. Perko, There are no unknown perfect binary codes, *Ann. Univ. Turku, Ser. A* I (1971), 148.